II

108TH CONGRESS
2D SESSION

S. 2481

To require that notices to consumers of health and financial services include information on the outsourcing of sensitive personal information abroad, to require relevant Federal agencies to prescribe regulations to ensure the privacy and security of sensitive personal information outsourced abroad, to establish requirements for foreign call centers, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 1, 2004

Mr. NELSON of Florida (for himself and Mrs. FEINSTEIN) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

To require that notices to consumers of health and financial services include information on the outsourcing of sensitive personal information abroad, to require relevant Federal agencies to prescribe regulations to ensure the privacy and security of sensitive personal information outsourced abroad, to establish requirements for foreign call centers, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ‘‘Increasing Notice of Foreign Outsourcing Act’’.

SEC. 2. HEALTH PRIVACY.

(a) FOREIGN-BASED BUSINESS ASSOCIATE.—In this section, the term ‘‘foreign-based business associate’’ means a business associate, as defined under the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note), whose operation is based outside the United States and that receives protected health information and processes such information outside the United States.

(b) NOTICES.—

(1) IN GENERAL.—The Secretary of Health and Human Services (referred to in this section as the ‘‘Secretary’’) shall revise the regulations prescribed pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note) to require a covered entity (as defined under such regulations and referred to in this section as a ‘‘covered entity’’), that outsources protected health information (as defined under such regulations and referred to in this section as ‘‘protected health information’’), outside the United

States to include in such entity's notice of privacy protections the following:

(A) The following information in simple language:

(i) Notification that the covered entity outsources protected health information to foreign-based business associates.

(ii) Any risks and consequences to the privacy and security of protected health information that arise as a result of the processing of such information outside the United States.

(iii) Additional measures the covered entity is taking to protect the protected health information outsourced for processing outside the United States.

(B) A certification that the covered entity has taken reasonable steps to ensure that the handling of protected health information will be done in compliance with applicable laws in all instances where protected health information is processed outside the United States, including the reasons for the certification.

(2) EFFECTIVE DATE.—A covered entity shall be required to include in such entity's notice of pri-

vacy protections the information and certification described in paragraph (1) for notices issued on or after the date on which the Secretary prescribes regulations pursuant to this section or the date that is 365 days after the date of enactment of this Act, whichever date is earlier. Nothing in this subsection shall be construed to require a covered entity to reissue notices issued before the date on which the Secretary prescribes regulations pursuant to this section or the date that is 365 days after the date of enactment of this Act, whichever date is earlier, to include in such notices the information and certification described in paragraph (1).

(c) RULEMAKING.—

(1) IN GENERAL.—

(A) REGULATORY AUTHORITY.—The Secretary shall—

(i) prescribe such regulations consistent with paragraph (2) as may be necessary to carry out this section with respect to foreign outsourcing; and

(ii) determine the appropriate penalties to impose upon a covered entity for a violation of a provision of this subsection or subsection (b).

(B) PROCEDURES AND DEADLINES.—The regulations described in subparagraph (A) shall be prescribed in accordance with all applicable legal requirements and shall be issued in final form not later than 365 days after the date of enactment of this Act.

(2) NECESSARY REGULATIONS.—The Secretary shall prescribe regulations—

(A) requiring that a contract between a covered entity and such entity's foreign-based business associate contain a provision that provides such entity with the right to audit such associate, as needed, to monitor performance under the contract; and

(B) requiring that foreign-based business associates and subcontractors of covered entities be contractually bound by Federal privacy standards and security safeguards.

(d) BREACH OF SECURITY.—

(1) BREACH OF SECURITY OF THE SYSTEM.—In this subsection, the term ''breach of security of the system''—

(A) means the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to protected health information maintained by the covered entity, foreign-based business associate, or subcontractor; and

(B) does not include good faith acquisition of protected health information by an employee or agent of the covered entity, foreign-based business associate, or subcontractor for the purposes of the entity, associate, or subcontractor, if the protected health information is not used or subject to further unauthorized disclosure.

(2) DATABASE SECURITY.—

(A) COVERED ENTITY.—A covered entity—

(i) that owns or licenses electronic data containing protected health information shall, following the discovery of a breach of security of the system containing such data, notify the Secretary of such breach; or

(ii) that receives a notification under subparagraph (B) of a breach, shall notify the Secretary of such breach.

(B) OTHER PARTIES.—

(i) THIRD PARTY.—The Secretary shall require that a contract between a covered entity and such entity's foreign-based business associate contain a provision that if the foreign-based business associate (or any subcontractor of such associate) owns or licenses electronic data containing protected health information that was provided to the associate through the covered entity, the associate (or subcontractor) shall, following the discovery of a breach of security of the system containing such data—

(I) notify the entity from which it received the protected health information of such breach; and

(II) provide a description to the entity from which it received the protected health information of any corrective actions taken to guard against future security breaches.

(ii) NOTIFICATION PROCESS.—Each entity that receives a notification under clause (i) shall notify the entity from which it received the protected health information of such breach until the notification reaches the foreign-based business associate who shall, in turn, notify the covered entity of such breach.

(C) TIMELINESS OF NOTIFICATION.—All notifications required under subparagraphs (A) and (B) shall be made as expediently as possible and without unreasonable delay following—

(i) the discovery of a breach of security of the system; and

(ii) any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.

(3) EFFECTIVE DATE.—This subsection shall take effect on the expiration of the date that is 365 days after the date of enactment of this subsection.

SEC. 3. FINANCIAL PRIVACY.

(a) FOREIGN-BASED BUSINESS.—Section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809) is amended by adding at the end the following:

"(12) FOREIGN-BASED BUSINESS.—The term 'foreign-based business' means a nonaffiliated third party whose operation is based outside the United

States and that receives nonpublic personal information and processes such information outside the United States.''.

(b) FINANCIAL NOTICES.—

(1) IN GENERAL.—Section 503(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6803(b)) is amended—

(A) in paragraph (3), by striking ''and'' after the semicolon;

(B) in paragraph (4), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(5) if the financial institution outsources nonpublic personal information outside the United States—

''(A) information informing the consumer in simple language—

''(i) that the financial institution outsources nonpublic personal information to foreign-based businesses;

''(ii) of any risks and consequences to the privacy and security of an individual's nonpublic personal information that arise as a result of the processing of such information outside the United States; and "(iii) of the additional measures the financial institution is taking to protect the nonpublic personal information outsourced for processing outside the United States; and

"(B) a certification that the financial institution has taken reasonable steps to ensure that the handling of nonpublic personal information will be done in compliance with applicable laws in all instances where nonpublic personal information is processed outside the United States, including the reasons for the certification.".

(2) EFFECTIVE DATE.—A financial institution shall include in such institution's disclosure the information and certification described in the amendment made by paragraph (1)(C) for disclosures provided on or after the date on which the regulatory agency that has jurisdiction over such institution pursuant to section 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6805) prescribes regulations pursuant to the amendments made by this section or the date that is 365 days after the date of enactment of this Act, whichever date is earlier. Nothing in this subsection, or the amendments made by this subsection, shall be construed to require a financial in-

stitution to reissue disclosures provided before the date on which the regulatory agency that has jurisdiction over such institution pursuant to section 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6805) prescribes regulations pursuant to the amendments made by this section or the date that is 365 days after the date of enactment of this Act, whichever date is earlier, to include in such disclosures the information and certification described in the amendment made by paragraph (1)(C).

(c) RULEMAKING.—Section 504 of the Gramm-Leach-Bliley Act (15 U.S.C. 6804) is amended by adding at the end the following:

"(c) RULEMAKING ON FOREIGN OUTSOURCING.—

"(1) IN GENERAL.—

"(A) REGULATORY AUTHORITY.—The Federal banking agencies, the National Credit Union Administration, the Secretary of the Treasury, the Securities and Exchange Commission, and the Federal Trade Commission (referred to in this subsection as the 'regulatory agencies') shall—

"(i) prescribe such regulations consistent with paragraph (2) as may be necessary to carry out this subtitle with respect to foreign outsourcing, with respect to the financial institutions subject to their jurisdiction under section 505; and

"(ii) determine the appropriate penalties to impose upon financial institutions for a violation of a provision of this subsection.

"(B) COORDINATION, CONSISTENCY, AND COMPARABILITY.—The regulatory agencies shall consult and coordinate with each other for the purposes of assuring, to the extent possible, that the regulations prescribed by each such agency are consistent and comparable with the regulations prescribed by the other such agencies.

"(C) PROCEDURES AND DEADLINES.—The regulations described in subparagraph (A) shall be prescribed in accordance with all applicable legal requirements and shall be issued in final form not later than 365 days after the date of enactment of this subsection.

"(2) NECESSARY REGULATIONS.—The regulatory agencies shall prescribe regulations—

"(A) requiring that a contract between a financial institution and such institution's foreign-based business contain a provision that provides such institution with the right to audit such business, as needed, to monitor performance under the contract; and

"(B) requiring that foreign-based businesses and subcontractors of financial institutions be contractually bound by Federal privacy standards and security safeguards.".

(d) BREACH OF SECURITY.—Section 502 of the Gramm-Leach-Bliley Act (15 U.S.C. 6802) is amended by adding at the end the following:

"(f) BREACH OF SECURITY.—

"(1) BREACH OF SECURITY OF THE SYSTEM.—In this subsection, the term 'breach of security of the system'—

"(A) means the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to nonpublic personal information maintained by the financial institution, foreign-based business, or subcontractor; and

"(B) does not include good faith acquisition of nonpublic personal information by an employee or agent of the financial institution, foreign-based business, or subcontractor for the purposes of the institution, business, or subcontractor, if the nonpublic personal information is not used or subject to further unauthorized disclosure.

"(2) DATABASE SECURITY.—

"(A) FINANCIAL INSTITUTION.—A financial institution—

"(i) that owns or licenses electronic data containing nonpublic personal information shall, following the discovery of a breach of security of the system containing such data, notify the entity under which the institution is subject to jurisdiction under section 505 of such breach; or

"(ii) that receives a notification under subparagraph (B) of a breach, shall notify the entity under which the institution is subject to jurisdiction under section 505 of such breach.

"(B) OTHER PARTIES.—

"(i) IN GENERAL.—The Federal banking agencies, the National Credit Union Administration, the Secretary of the Treasury, the Securities and Exchange Commission, and the Federal Trade Commission shall require, with respect to the financial institutions subject to their jurisdiction under section 505, that a contract between a financial institution and such institution's foreign-based business contain a provision that if the foreign-based business (or any subcontractor of such business) owns or licenses electronic data containing nonpublic personal information that was provided to the business through the financial institution, the business (or subcontractor) shall, following the discovery of a breach of security of the system containing such data—

"(I) notify the entity from which it received the nonpublic personal information of such breach; and

"(II) provide a description to the entity from which it received the nonpublic personal information of any corrective actions taken to guard against future security breaches.

"(ii) NOTIFICATION PROCESS.—Each entity that receives a notification under clause (i) shall notify the entity from which it received the nonpublic personal information of such breach until the notification reaches the foreign-based business who shall, in turn, notify the financial institution of such breach.

"(C) TIMELINESS OF NOTIFICATION.—All notifications required under subparagraphs (A) and (B) shall be made as expediently as possible and without unreasonable delay following—

"(i) the discovery of a breach of security of the system; and

"(ii) any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.

"(3) EFFECTIVE DATE.—This subsection shall take effect on the expiration of the date that is 365 days after the date of enactment of this subsection.".

SEC. 4. FOREIGN CALL CENTERS.

(a) FOREIGN CALL CENTER DEFINED.—In this section, the term ''foreign call center'' means a foreign-based service provider or a foreign-based subcontractor of such provider that—

(1) is unaffiliated with the entity that utilizes such provider or subcontractor; and

(2) provides customer-based service and sales or technical assistance and expertise to individuals located in the United States via the telephone, the Internet, or other telecommunications and information technology.

(b) REQUIREMENT.—A contract between a foreign call center and an entity that utilizes such foreign call center to initiate telephone calls to, or receive telephone calls from, individuals shall include a requirement that each employee of the foreign call center disclose the physical location of such employee upon the request of such individual.

(c) CERTIFICATION REQUIREMENT.—An entity described in subsection (b) shall submit an annual certification to the Federal Trade Commission on whether or not the entity and its subsidiaries, and the foreign call center employees and its subsidiaries, have complied with subsection (b). Such annual certifications shall be made available to the public.

(d) NONCOMPLIANCE.—An entity described in subsection (b) or its subsidiaries that violates subsection (b) shall be subject to such civil penalties as the Federal Trade Commission prescribes under subsection (e).

(e) REGULATIONS.—Not later than 365 days after the date of enactment of this Act, the Federal Trade Commission shall prescribe such regulations as are necessary for effective monitoring and compliance with this section. Such regulations shall include appropriate civil penalties for noncompliance with this section.